

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between; align-items: flex-end;"> <div style="width: 30%;"> <p>Date: _____</p> </div> <div style="width: 65%;"> <div style="text-align: center; margin-bottom: 10px;"> <p>_____</p> <p><i>Executing officer's signature</i></p> </div> <div style="text-align: center;"> <p>_____</p> <p><i>Printed name and title</i></p> </div> </div> </div>		

ATTACHMENT A

The property to be searched is described as follows:

- a. Item A: White Apple I-Phone touch screen cell phone obtaining Serial Number: FFMSG46AGRY3. Investigators located the white Apple I-Phone at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227.
- b. Item B: Blue Apple I-phone touch screen cell phone with black case. Investigators located the blue Apple I-Phone at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227.
- c. Item C: Night Owl Surveillance Digital Video Recorder (DVR). Investigators located the Night Owl Surveillance DVR at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227.
- d. Item D: Black Wiko touch screen cell phone. Investigators located the black Wiko cell phone at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227.
- e. Item E: Red, silver, and black Android touch screen cell phone. Investigators located the red, silver, and black Android cell phone at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227.
- f. Item F: Black Dell Lap Top Computer. Investigators located the black Dell Computer at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227.
- g. Item G: Silver Apple Mac Book Pro Lap Top Computer. Investigators located the silver Apple Mac Book at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227.
- h. Item H: Green Apple I-Phone Touch Screen Cell Phone with black case. Investigators located the Green Apple I-Phone cell phone at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227.

- i. Item I: Gold Samsung Galaxy S7 Touch Screen Cell Phone with black case. Investigators located the gold Samsung Galaxy S7 cell phone at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227.
- j. Item J: Blue Alcatel flip phone. Investigators located the blue Alcatel flip phone at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227.
- k. Item K: Blue Samsung Verizon flip phone Model # SM-B690V. Investigators located the blue Samsung Verizon flip phone at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227.
- l. Item L: Blue Samsung Cricket Touch Screen Cell Phone. Investigators located the blue Samsung Cricket Cell Phone at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227.

ATTACHMENT B

1. All records on the **ELECTRONIC DEVICES** described in Attachment A that relate to violations of Title 21, United States Code, Sections 841(a)(1), 846, and 843(b), Distribution of, and Possession with Intent to Distribute, Controlled Substances and violations of under Title 18, and Title 49, United States Code, including 18 U.S.C. § 513 (possession of a forged or counterfeit security); 18 U.S.C. § 1341 (mail fraud), 18 U.S.C. § 371 (conspiracy), 49 U.S.C. 32703(2) (odometer tampering), and 49 U.S.C. § 32705(a)(2) (false odometer disclosure statements).

- a. Contact lists;
- b. Any information regarding schedules or travel;
- c. All bank records. Checks, credit card bills, account information, and other financial records;
- d. Photographs and/or video depicting drug trafficking, money laundering, or other related activity, including co-conspirators and/or others engaged in such activity; and
- e. Records of Internet Protocol (IP) addresses used; records of internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any internet search engine, and records of user typed web addresses.

2. Evidence of user attribution showing who used or owned the **ELECTRONIC DEVICES** at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Electronic Devices A-L, currently in the law
enforcement possession, as further described in
Attachment A.

Case No.22-955M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the _____ Eastern _____ District of _____ Wisconsin _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. §841(a)(1); 846&843	Possession, distribution, and conspiracy to possess and distribute controlled
(b); 18 U.S.C. §513, 371; 49	substances; Possession of a forged or counterfeit security; Mail Fraud;
U.S.C. §32703(2), 32705(a)(2)	Conspiracy; Odometer tampering and False odometer disclosure statements.

The application is based on these facts:

See Attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

SEAN MAYERBOCK (Affiliate) Digitally signed by SEAN MAYERBOCK (Affiliate)
Date: 2022.08.15 08:06:36 -05'00'

Applicant's signature

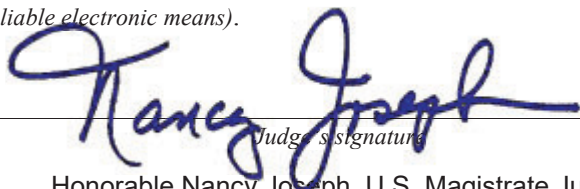
HIDTA TFO Sean Mayerbock

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
_____ telephone _____ (specify reliable electronic means).

Date: 8/16/2022

City and state: Milwaukee, Wisconsin


Judge's signature

Honorable Nancy Joseph, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER
RULE 41 FOR A WARRANT TO SEARCH AND SEIZE**

I, Sean Mayerbock, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

I, Task Force Officer Sean Mayerbock, being first duly sworn, hereby depose and state as follows:

1. I am a Police Officer with the City of Brookfield Police Department and have been a sworn law enforcement officer for 7 years. I am currently assigned to the North Central High Intensity Drug Trafficking Area (HIDTA) – Drug Gang Task Force. Since November 2019, I have been a Task Force Officer with the United States Department of Justice, Drug Enforcement Administration.

2. I am familiar with various methods of smuggling and trafficking controlled substances and their proceeds. I am also familiar with methods used to by traffickers to evade detection of both the controlled substances and its' proceeds. I have received training in the investigation of and am knowledgeable in investigations pertaining to drug trafficking, illegal firearm possession and trafficking, money laundering, financial investigations, and various methods which drug dealers use in an effort to conceal and launder the proceeds of their illicit drug trafficking enterprises.

3. I have received training in the area of narcotics investigations, money laundering, financial investigations, and various methods that drug dealers use in an effort to conceal and launder the proceeds of their illicit drug trafficking enterprises. I have participated in numerous investigations involving violations of state and federal narcotics laws. I have participated or assisted in numerous federal search warrants for narcotic related offenses, which have resulted in

the seizure of controlled substances, firearms, United States currency, vehicles, real estate, and jewelry from individuals involved in narcotic trafficking.

4. I have extensive training and experience in the investigation of Drug Trafficking Organizations (DTO). I am familiar with the different structures, the motivations for criminal their activities, the hierarchies, and the variety of roles of the members within the organizations. I have applied my training in the investigation of these organizations and have charted and tracked them. My investigations have revealed the geographical locations that they inhabit, the level of violence and crimes they have committed and their hierarchy and the roles of their members within their respective organizations. I have participated in these types of investigations as both the lead investigator and co-agent and have successfully dismantled them by use of several law enforcement investigation techniques to include wiretaps.

5. In addition, through training, experience, and discussions with other experienced agents:

- a. I have learned about the manner in which individuals and organizations distribute controlled substances;
- b. I am familiar with the appearance and street names of various drugs, including marijuana, heroin, cocaine, and crack cocaine. I am familiar with the methods used by drug dealers to package and prepare controlled substances for sale. I know the street values of different quantities of the various controlled substances;
- c. I am familiar with the coded language utilized over the telephone to discuss drug trafficking and know that the language is often limited, guarded, and coded. I also know the various code names used to describe controlled substances;

- d. I know drug dealers often put telephones in the names of others (nominees) or obtain pre-paid cellular telephones from companies where no subscriber name or address is required to distance themselves from telephones that they use to facilitate drug distribution. Because drug traffickers go through many telephone numbers, they often do not pay final bills when they are done using a telephone number and then are unable to put another line in the name of that subscriber;
- e. I know large-scale drug traffickers often purchase and/or title their assets in fictitious names, aliases or the names of relatives, associates, or business entities to avoid detection of these assets by government agencies. I know that even though these assets are in names other than the drug traffickers, the drug traffickers actually own and continue to use these assets and exercise dominion and control over them;
- f. I know large-scale drug traffickers must maintain on-hand, large amounts of U.S. currency to maintain and finance their ongoing drug business;
- g. I know it is common for drug traffickers to maintain books, records, receipts, notes, ledgers, airline tickets, receipts relating to the purchase of financial instruments and/or the transfer of funds and other papers relating to the transportation, ordering, sale and distribution of controlled substances. That the aforementioned books, records, receipts, notes, ledgers, etc., are maintained where the traffickers have ready access to them;

- h. I know it is common for large-scale drug traffickers to secrete contraband, proceeds of drug sales and records of drug transactions in secure locations within their residences, their businesses and/or other locations over which they maintain dominion and control, for ready access and to conceal these items from law enforcement authorities or rival drug traffickers. These secure locations include, but are not limited to, safes, briefcases, purses, locked filing cabinets, and hidden storage areas in natural voids of a residence;
- i. I know it is common for persons involved in large-scale drug trafficking to maintain evidence pertaining to their obtaining, secreting, transfer, concealment, and/or expenditure of drug proceeds, such as currency, financial instruments, precious metals and gemstones, jewelry, books, records of real estate transactions, bank statements and records, passbooks, money drafts, letters of credit, money orders, bank drafts, cashier's checks, bank checks, safe deposit box keys and money wrappers. These items are maintained by the traffickers within residences (including attached and unattached garages, and outbuildings), businesses or other locations over which they maintain dominion and control;
- j. I know large-scale drug traffickers often use electronic equipment such as telephones (landlines and cell phones), computers, telex machines, facsimile machines, currency counting machines and telephone answering machines to generate, transfer, count, record and/or store the information described in the items above, as well as conduct drug trafficking activities;

- k. I know when drug traffickers amass large proceeds from the sale of drugs, the drug traffickers attempt to legitimize these profits through money laundering activities. To accomplish these goals, drug traffickers utilize the following methods, including, but not limited to: domestic and international banks and their attendant services, securities brokers, professionals such as attorneys and accountants, casinos, real estate, shell corporations and business fronts, and otherwise legitimate businesses that generate large quantities of currency;
- l. I know drug traffickers commonly maintain addresses or telephone numbers in books or papers that reflect names, addresses and/or telephone numbers of their associates in the trafficking organization;
- m. I know drug traffickers take or cause to be taken photographs of themselves; their associates, their property and their drugs. These traffickers usually maintain these photographs in their possession;
- n. I know a “controlled buy” (and/or controlled contact) is a law enforcement operation in which an informant purchases drugs from a target. The operation is conducted using surveillance, usually audio and video taping equipment, and pre-recorded buy money. When an informant is used, he/she is searched for contraband, weapons, and money before the operation. The informant is also wired with a concealed body recorder and monitoring device. When the transaction is completed, the informant meets case agents at a pre-determined meet location and gives the purchased drugs and the recording/monitoring equipment to the case agents. The informant is again searched for contraband, weapons, and

money. Additionally, all telephone calls made by the informant while under the direction and control of case agents are recorded;

- o. During the course of residential searches, I and other agents have also found items of personal property that tend to identify the person(s) in residence, occupancy, control, or ownership of the subject premises. Such identification evidence is typical of the articles people commonly maintain in their residences, such as canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, utility and telephone bills, statements, identification documents, and keys.

6. Pursuant to my official duties, I am submitting this affidavit in support of an application for a search warrant for violations of federal laws, including violations of Title 21, United States Code, Sections 841(a)(1), 846, and 843(b), Distribution of, and Possession with Intent to Distribute, Controlled Substances and violations of under Title 18, and Title 49, United States Code, including 18 U.S.C. § 513 (possession of a forged or counterfeit security); 18 U.S.C. § 1341 (mail fraud), 18 U.S.C. § 371 (conspiracy), 49 U.S.C. 32703(2) (odometer tampering), and 49 U.S.C. § 32705(a)(2) (false odometer disclosure statements).

7. I am personally involved in the investigation of the offenses discussed in this affidavit and I am familiar with all aspects of this investigation. The statements contained in this affidavit are based on my knowledge and, in part, information provided by LEOs, including (a) my personal knowledge and observations derived from participation in this investigation; (b) review of oral and written reports that I have received directly or indirectly from other LEOs about this and other drug-trafficking investigations; (c) discussions I personally had concerning this investigation with other experienced drug-trafficking Case Agents; (d) physical surveillance

by the DEA, Homeland Security Investigations (HSI), and local law enforcement agencies, the results of which have been reported to me directly or indirectly; (e) public records; (f) review of telephone toll records, pen register and trap and trace information, and telephone subscriber information; (g) information provided by confidential sources working for the DEA, HSI, and North Central HIDTA; (h) consensually-recorded phone calls between confidential sources, and undercover agents; (i) controlled purchases of heroin, fentanyl; (j) review of driver's license and automobile registration records; (k) records obtained from law enforcement databases; (l) my training and experience as a DEA TFO; and (m) the training and experience of other LEOs involved in this investigation.

8. The statements in this affidavit are based on my personal knowledge, and on information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts. Because this affidavit is being submitted for the limited purpose of securing search warrants, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations set forth above occurred and that probable cause exists to believe that the property described in Attachment A, incorporated herein by reference, contain the items that are described in Attachment B.

ELECTRONIC DEVICES FOR WHICH SEARCH WARRANTS ARE SOUGHT

9. For the reasons discussed herein, there is probable cause to believe that located in the following **ELECTRONIC DEVICES** more fully described in Attachment A, are items that constitute evidence of drug trafficking and fraud, including violations of under Title 18, Title 49,

and Title 21 United States Code, including 18 U.S.C. § 513 (possession of a forged or counterfeit security); 18 U.S.C. § 1341 (mail fraud), 18 U.S.C. § 371 (conspiracy), 49 U.S.C. 32703(2) (odometer tampering), 49 U.S.C. § 32705(a)(2) (false odometer disclosure statements) and 21 U.S.C, Section 841(a)(1) and 846 843(b). (Distribution of, and Possession with Intent to Distribute, Controlled Substances)

- a)** White Apple I-Phone touch screen cell phone obtaining Serial Number: FFMSG46AGRY3. Investigators located the white Apple I-Phone at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227. (Device A).
- b)** Blue Apple I-phone touch screen cell phone with black case. Investigators located the blue Apple I-Phone at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227. (Device B).
- c)** Night Owl Surveillance Digital Video Recorder (DVR). Investigators located the Night Owl Surveillance DVR at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227. (Device C).
- d)** Black Wiko touch screen cell phone. Investigators located the black Wiko cell phone at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227. (Device D).
- e)** Red, silver, and black Android touch screen cell phone. Investigators located the red, silver, and black Android cell phone at 8018 W. Hope St., Milwaukee, WI.

Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227. (Device E).

- f)** Black Dell Lap Top Computer. Investigators located the black Dell Computer at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227. (Device F).
- g)** Silver Apple Mac Book Pro Lap Top Computer. Investigators located the silver Apple Mac Book at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227. (Device G).
- h)** Green Apple I-Phone Touch Screen Cell Phone with black case. Investigators located the Green Apple I-Phone cell phone at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227. (Device H).
- i)** Gold Samsung Galaxy S7 Touch Screen Cell Phone with black case. Investigators located the gold Samsung Galaxy S7 cell phone at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227. (Device I).
- j)** Blue Alcatel flip phone. Investigators located the blue Alcatel flip phone at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227. (Device J).
- k)** Blue Samsung Verizon flip phone Model # SM-B690V. Investigators located the blue Samsung Verizon flip phone at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227. (Device K).

- I) Blue Samsung Cricket Touch Screen Cell Phone. Investigators located the blue Samsung Cricket Cell Phone at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227. (Device L).

FEDERAL SEARCH WARRANTS ON GREGORY HAYES DTO

10. Based on the above-referenced evidence, on July 7, 2022, the Honorable US Magistrate Judge Stephen C. Dries signed and authorized seven federal search warrants for the following locations: 7704 W. Appleton Ave. Milwaukee, WI, Auto Source LLC (associated to Gregory HAYES), 8018 W. Hope Ave., Milwaukee, WI (associated to Gregory HAYES), 2323 N. 37th Street Milwaukee, WI (associated to Calvin COLEMAN), 4626 N. 52nd Street, Milwaukee, WI (associated to Calvin COLEMAN), 3419 N. 56th Street, Milwaukee, WI (associated to Edward YOUNGBLOOD), 103 E. Burleigh Street, Milwaukee, WI (associated to Robert WOODS), and 5555 N. 27th Street, Milwaukee, WI Parking Stall P6 and Storage Unit A56 (associated to John FERGUSON and the fraudulent cashier check investigation).

11. On July 12, 2022, at approximately 6:00AM, case agents coordinated the execution of all seven search warrants. The following is a summary of the executed federal search warrants. At 7704 W. Appleton Ave. (Auto Source LLC owned by Gregory HAYES), investigators recovered multiple documents related to the fraud/odometer investigation, financial documentation, vehicle titles, electronic evidence, and approximately 475 grams of marijuana. No subjects at this location were taken into custody and Gregory HAYES was not present at this location at the time of the search warrant.

12. At 4626 N. 52nd Street (associated to Calvin COLEMAN) investigators recovered multiple cell phones, various documents related to the fraud/odometer investigation, vehicle titles,

approximately 56 grams cocaine, approximately 1.5 grams of fentanyl, approximately 36 grams of MDMA, .64 grams of heroin and a large sum of US Currency. Residing at the residence was Calvin COLEMAN, Seconi MATHEWS F/B 06/10/1979, and three juveniles. Both COLEMAN and MATHEWS were taken into custody.

13. At 2323 N. 37th Street investigators recovered various documents. No subjects were taken into custody at this location.

14. At 103 E. Burleigh Street, (Merrywood Auto owned by Robert WOODS) investigators recovered multiple documents related to the fraud/odometer investigation, financial documentation, vehicle titles, and electronic evidence. No subjects were taken into custody and Robert WOODS was not located at the business.

15. At 5555 N. 27th Street, parking stall P6 and Storage unit A56 (related to the fraud investigation) investigators recovered a stolen 1999 Coach Man 40ft RV in parking stall P6. Inside the Storage unit investigators recovered a cell phone, a digital scale, and a glass Pyrex measuring cup. No subjects were taken into custody at this location.

16. At 3419 N. 56th Street (known residence of Edward YOUNGBLOOD), investigators recovered a cell phone, a computer, five stolen vehicles (related to the fraud investigation), five firearms with various types of ammunition, approximately 850 grams of cocaine, approximately 1.5 grams of heroin, approximately 4 grams of methamphetamine, approximately 130 grams of marijuana, digital scales, multiple vehicle key fobs/keys, counterfeit currency, multiple documents related to the fraud investigation, WI DOT documentation, and multiple blank printed cashier's checks. Residing at the residence was Edward YOUNGBLOOD, Shanteah RILEY F/B 02/15/1989, and a juvenile. YOUNGBLOOD was taken into custody by investigators.

17. The five stolen vehicles were towed and returned to their rightful owners. On July 18, 2022, case agents were made aware by the owner of one of the stolen vehicles (black, 1968, Oldsmobile convertible, VIN #336678M322975, that was originally located inside the garage of 3419 N. 56th Street) that they located a cell phone inside of the vehicle and the phone did not belong to them. Jefferson County Sheriff's Office Detective Donald Petig recovered the red Apple I-phone who ultimately turned the phone over to case agents.

18. At 8018 W. Hope Ave., (known residence of Gregory HAYES) investigators recovered numerous documents related to the on-going theft/fraud investigation, six firearms, approximately 27.8 grams of cocaine, approximately 1,611.08 grams of marijuana, 11 Lorazepam pills, 6 Oxycodone pills. Additionally located at the residence were **Items A - L**. Residing at the residence was Theresa HAYES-WIMBERLY F/B 06/14/51, Larry C. HAYES M/B 12/05/37, Gregg W. HAYES M/B 10/13/88, Isaiah D. JACKSON M/B 09/17/92, and two juveniles. Both Gregg W. HAYES and Isaiah D. JACKSON were taken into custody by investigators. Gregory HAYES was not located at the location. During the investigation, the premises of 134 East Chateau Place, Whitefish Bay, WI, was identified as being associated with HAYES. The mother of HAYES' child, Nichole L. TURNER, black female, DOB: 11-07-85, was identified as residing at the location. A team of investigators were assigned as a "knock and talk" team at the 134 East Chateau Place, Whitefish Bay, WI tasked with conducting a knock and talk at 134 East Chateau Place. The knock and talk would be conducted after the aforementioned search warrants were executed by other investigators. After the execution of the search warrant at 8018 W. Hope, case agents informed the "knock and talk" team that Gregory HAYES was not at the residence. Investigators at 134 East Chateau Place observed a blue Honda Odyssey van bearing Wisconsin Dealer plate MV5567H, parked on the street in front of 134 East

Chateau Place. A check revealed the plate was not associated to a vehicle, but the owner was Auto Source LLC (Gregory HAYES' auto shop).

19. Approximately two hours after the execution of the search warrants, the knock and talk was executed at 134 East Chateau Place. While ringing the doorbell, investigators observed the blinds on the 2nd floor move, indicating someone looked outside. Investigators continued to ring the doorbell and knock on the door. After not receiving a response, investigators began to announce their presence while asking TURNER to speak with investigators. Investigators did not receive any response. Approximately 10 minutes later, investigators called TURNER's cellular phone (414-531-7188) and spoke with TURNER. During the conversation investigators advised TURNER that HAYES was wanted by law enforcement. TURNER acknowledged knowing HAYES was inside the residence and advised investigators HAYES would come to the door. A few minutes later TURNER opened a 2nd floor window and advised investigators that HAYES was coming to the door. A short time later, HAYES came to the door and was subsequently taken into custody. After HAYES was taken into custody, investigators advised TURNER that case agents were applying for a search warrant and inquired who was inside the residence. TURNER informed investigators her (2) children were in the residence. Investigators informed TURNER that case agents needed to secure the residence for the search warrant. TURNER informed investigators that she wasn't going to allow investigators into the residence. During the conversation TURNER informed investigators that she was concerned because her children were in the home. TURNER agreed to let investigators into the residence to secure the residence after her children were turned over to her sister "Brittany".

20. TURNER walked away from investigators to retrieve the children. TURNER returned to the door a short time later with a baby and child. TURNER also had a black bag slung over her shoulder. Investigators advised TURNER that they couldn't allow the bag to leave the residence.

TURNER was upset that investigators wouldn't allow the "baby's book bag" to leave the residence. During their conversation, TURNER turned and walked away from investigators while stating "let me get my money out of here". TURNER went on to state she had money in the bag. Fearing that TURNER was going to destroy evidence, investigators entered the residence and attempted to take TURNER into custody and secure the bag. TURNER became uncooperative with investigators and began to attempt to pull away. TURNER was yelling at investigators and wouldn't allow officers to place her into handcuffs. TURNER was subsequently directed to the ground and taken into custody.

21. On July 12, 2022, at approximately 2:35PM, the Honorable US Magistrate Judge Stephen C. Dries signed and authorized a search warrant for 134 East Chateau Place, Whitefish Bay, WI. Located within the residence was multiple cell phones, three firearms, 1.65 grams of methamphetamine, a large sum of US Currency (located in the bag TURNER attempted to turn over to her sister "Brittany," previously referenced, and inside of the residence), firearm ammunition, and various documents related to the fraud/odometer investigation.

22. Based upon the above-detailed facts, there is probable cause to believe that a search of the information contained within the above-described **ELECTRONIC DEVICES** will produce evidence of a crime; namely, evidence related to Distribution of, and Possession with Intent to Distribute, Controlled Substances, possession of a forged or counterfeit security, mail fraud, odometer tampering, and false odometer disclosure statements. Through your affiant's training, experience and discussions with other experienced law enforcement officers, your affiant is familiar with the ways in which drug traffickers conduct their unlawful trade, including their methods of distribution, their utilization of communication devices, their use of coded communications to conduct their transactions, the employment of counter surveillance, their use of false or fictitious identities, and their utilization of various forms of **ELECTRONIC DEVICES** to store and/or conceal illegal activity.

23. Based upon my training and experience, your affiant knows that individuals involved in drug trafficking frequently use cellular telephones to maintain contact with their drug sources as well as customers and co-conspirators in the distribution of controlled substances; that individuals involved in drug trafficking often use multiple cellular telephones to compartmentalize their illicit activity to help evade detection by law enforcement; that your affiant has also found it very common for crime suspects to use their cellular telephones to communicate aurally or via electronic message in “text” format with individuals whom they purchase, trade, or otherwise negotiate to obtain illegal drugs; therefore records contained within said **ELECTRONIC DEVICES** will provide evidence related to the identity of said supplier(s), coconspirators, and customers.

24. Based upon my training and experience, your affiant believes it is common for individuals who possess illegal drugs to often take or cause to be taken photographs and other visual depictions of themselves, their associates, and the illegal drugs that they control, possess, buy, and sell; furthermore, your affiant believes it is common for these photographs and visual depictions to be kept and maintained on their cellular devices.

25. Your affiant knows that the **ELECTRONIC DEVICES** have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the **ELECTRONIC DEVICES** first came into the possession of case agents.

TECHNICAL TERMS

26. Based on my training and experience, I use the following technical terms to convey the following meanings

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of

transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic films. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to

store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

- f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.
- g. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- h. Internet: The Internet is a global network of computers and other **ELECTRONIC DEVICES** that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

27. Based on training, experience, and research, your affiant knows that the **ELECTRONIC DEVICES** have the capabilities that allow them to serve as wireless telephones, digital cameras, portable media players, GPS navigation devices, and PDAs. Others of the devices, such as the DVR system, are capable of capturing video, photographs, and audio. In my training and

experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the devices.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

10. Based on knowledge, training, and experience, your affiant knows that **ELECTRONIC DEVICES** can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

11. There is probable cause to believe that things that were once stored on the **ELECTRONIC DEVICES** may still be stored there, for at least the following reasons:

- a. Based on knowledge, training, and experience, your affiant knows that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

12. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **ELECTRONIC DEVICES** were used, the purpose their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the **ELECTRONIC DEVICES** because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other

external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how **ELECTRONIC DEVICES** were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

13. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant your affiant is applying for would permit the examination of the **ELECTRONIC DEVICES** consistent with the warrant. The examination may require authorities to employ

techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

14. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, your affiant submits there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

15. Your affiant submits that this affidavit supports probable cause for a search warrant authorizing the examination of the **ELECTRONIC DEVICES** described in Attachment A to seek the items described in Attachment B.

ATTACHMENT A

The property to be searched is described as follows:

- a. Item A: White Apple I-Phone touch screen cell phone obtaining Serial Number: FFMSG46AGRY3. Investigators located the white Apple I-Phone at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227.
- b. Item B: Blue Apple I-phone touch screen cell phone with black case. Investigators located the blue Apple I-Phone at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227.
- c. Item C: Night Owl Surveillance Digital Video Recorder (DVR). Investigators located the Night Owl Surveillance DVR at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227.
- d. Item D: Black Wiko touch screen cell phone. Investigators located the black Wiko cell phone at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227.
- e. Item E: Red, silver, and black Android touch screen cell phone. Investigators located the red, silver, and black Android cell phone at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227.
- f. Item F: Black Dell Lap Top Computer. Investigators located the black Dell Computer at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227.
- g. Item G: Silver Apple Mac Book Pro Lap Top Computer. Investigators located the silver Apple Mac Book at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227.
- h. Item H: Green Apple I-Phone Touch Screen Cell Phone with black case. Investigators located the Green Apple I-Phone cell phone at 8018 W. Hope St.,

Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227.

- i. Item I: Gold Samsung Galaxy S7 Touch Screen Cell Phone with black case. Investigators located the gold Samsung Galaxy S7 cell phone at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227.
- j. Item J: Blue Alcatel flip phone. Investigators located the blue Alcatel flip phone at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227.
- k. Item K: Blue Samsung Verizon flip phone Model # SM-B690V. Investigators located the blue Samsung Verizon flip phone at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227.
- l. Item L: Blue Samsung Cricket Touch Screen Cell Phone. Investigators located the blue Samsung Cricket Cell Phone at 8018 W. Hope St., Milwaukee, WI. Currently located at the West Allis Police Department at 11301 W. Lincoln Ave., West Allis, WI 53227.

ATTACHMENT B

1. All records on the **ELECTRONIC DEVICES** described in Attachment A that relate to violations of Title 21, United States Code, Sections 841(a)(1), 846, and 843(b), Distribution of, and Possession with Intent to Distribute, Controlled Substances and violations of under Title 18, and Title 49, United States Code, including 18 U.S.C. § 513 (possession of a forged or counterfeit security); 18 U.S.C. § 1341 (mail fraud), 18 U.S.C. § 371 (conspiracy), 49 U.S.C. 32703(2) (odometer tampering), and 49 U.S.C. § 32705(a)(2) (false odometer disclosure statements).

- a. Contact lists;
- b. Any information regarding schedules or travel;
- c. All bank records. Checks, credit card bills, account information, and other financial records;
- d. Photographs and/or video depicting drug trafficking, money laundering, or other related activity, including co-conspirators and/or others engaged in such activity; and
- e. Records of Internet Protocol (IP) addresses used; records of internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any internet search engine, and records of user typed web addresses.

2. Evidence of user attribution showing who used or owned the **ELECTRONIC DEVICES** at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.